

REMARKS/ARGUMENTS

Substance of interview. The Interview Summary requires that the undersigned include within this response the "substance of the interview". What follows is the substance of the recent telephone interviews regarding the IDS.

On July 23, 2004 the undersigned received the Office Action dated July 20, 2004, and noted that the Examiner had not considered the IDS filed in 2001. On August 18, 2004, the undersigned spoke with the Examiner to ask why the IDS had not been considered. On that day, at the Examiner's request, the undersigned faxed a copy of the IDS, not including the references which were voluminous. On October 21, 2004 the undersigned faxed a repeated request that the IDS be considered. On October 19, 2004 and October 21, 2004 the undersigned telephoned the Examiner to request that the IDS be considered, leaving voice mail messages on each day. On November 3, 2004 the undersigned sent an entire second copy of the IDS (including all references) in a package weighing 13 pounds. This IDS was received by the USPTO on November 4, 2004. The undersigned telephoned the Examiner on December 8, 2004, December 9, 2004, December 10, 2004, and December 13, 2004, leaving voice mail messages asking that the IDS be considered. On December 13, 2004, the undersigned and the Examiner conferred by telephone, and in this conference the Examiner declined to consider the IDS until the next Office Action. On December 14, 2004, the undersigned telephoned the Examiner's supervisor, Examiner Vu, leaving a telephone message asking that the IDS be considered. On December 15, 2004, Examiner Vu and the undersigned conferred by telephone, and it was agreed that the IDS would be considered presently. On December 20, 2004, the Examiner considered the IDS and faxed it (with initials and signature) to the undersigned, along with an interview summary record.

Applicant thanks the Examiner for his courtesy in now considering the IDS which was originally filed in 2001 but which was apparently lost within the Patent Office.

The **First Issue** is whether the Examiner is justified in rejecting claims 1-3 and 9-11 under 35 USC 103(a) as being unpatentable over Kalajan (US/6304908), hereinafter Kalajan, despite:

(1-a) Kalajan's failure to disclose

(1-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol,

(1-a-2) configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, and

(1-a-3) configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443;

(1-b) Kalajan's teaching away from

(1-b-1) providing to clients information about the IP address and host port number of secure hypertext transport servers;

(1-c) the fact that

(1-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(1-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(1-c-3) during the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem as defined below at 1-c (i.e., how to communicate securely through a firewall that blocks outgoing packets with a destination port of 443),

(1-c-4) the Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server, and

(1-c-5) the Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was

confronted by the Firewall Problem; and

(1-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

To understand the following discussion, it is useful to remember that when a web browser program running on a client computer sends to a web host computer a packet requesting a new session, the sent packet typically includes, among other things, the following four elements:

Name	Description
Source IP Address	The IP address that has been assigned to the client computer. In the simplest case, when the client computer and the host computer are connected directly to the Internet without any firewall or network address translation, this will be a valid, routable IP address.
Source Port	This is the port number on which the client computer will listen for a response to the request set forth in the body of the sent packet. If a client computer wishes to have multiple simultaneous sessions with one or more hosts, the client computer will typically pick a different Source Port for each session. Doing so will allow the client computer to easily figure out the applicable session for each received packet.
Destination IP Address	The IP address to which the packet is being sent. In the simplest case, when the client computer and the host computer are connected directly to the Internet without any firewall or network address translation, this will be a valid, routable IP address.
Destination Port	<p>This is the port number where the client computer hopes the host will be listening for session requests of the type that the client computer is making in the sent packet.</p> <p>Normally, if the client computer wishes to establish a HTTP session with the host, the client computer will specify a Destination Port of 80. Note that for many browser programs a URL of the form http://www.domain.com implies port 80 and is equivalent to a URL of the form http://www.domain.com:80</p> <p>Normally, if the client computer wishes to establish a HTTPS session with the host, the client computer will specify a Destination Port of 443. Note that for many browser programs a URL of the form https://www.domain.com implies port 443 and is</p>

	equivalent to a URL of the form https://www.domain.com:443
--	--

Some client computers are connected to the Internet through firewalls that are configured to pass outgoing packets to any Destination IP Address if the Destination Port is 80, but to block (i.e., not pass) outgoing packets to any Destination IP Address if the Destination Port is 443.

One embodiment of Applicant's invention concerns configuring a web server to listen for requests for HTTPS sessions on port 80 (rather than port 443) and then directing a web browser to send requests for HTTPS sessions to port 80 (rather than port 443), thereby permitting encrypted communications through firewalls of the type described above. For example, directing a browser to request a URL of the form https://www.domain.com:80.

On the other hand, Kalajan's invention relates generally to hiding host computers behind Kalajan's server 18, which redirects received packets based upon the Source IP Address (14a, 14b or 14c) and, if multiple clients share a single Source IP Address as can happen when clients are connected to the internet through a network address translation server, the Source Port number (12a, 12b or 12c). Kalajan's invention restricts which client computers can access a host, and hides from the client computers the IP addresses (valid or invalid) that are used by Kalajan's Hosts 1, 2 and 3. Before a client computer can access Kalajan's Host 1, 2 or 3, the client computer's IP address must be entered in Kalajan's address mapping table 38.

(1-a) Kalajan fails to disclose elements of claims 1-3 and 9-11.

(1-a-1) Kalajan fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by (i) Claim 1 step (a) (upon which claims 2-3 and 9 depend), (ii) Claim 10 step (a) and (iii) Claim 11 element (a).

The Examiner has failed to suggest any mapping between the elements of

Kalajan's disclosure and the elements of Applicant's invention. After reviewing Kalajan, Applicant believes that the following mapping makes the most sense, in the context of Claims 1-3 and 9-11:

Element of Kalajan's Disclosure	Element of Applicant's Invention
A program running on Kalajan's Host 1 (28a), Host 2 (28b) and/or Host 3 (28c)	Server Program using a secure hypertext transfer protocol
Kalajan's Host 1 port number (31a), Host 2 port number (31b) and/or Host 3 port number (31c)	Port number on which the Server Program Listens for requests for secure hypertext transfer protocol sessions
A program running on Kalajan's Client A (10a), Client B (10b) and/or Client C (10c)	Client Program
Kalajan's Server (18), which redirects packets based upon the source address of the client that sent the packet to the Server	No corresponding element in Claims 1-3 or 9-11. For purposes of Claims 1-3 and 9-11, Kalajan's Server 18 would be replaced with a piece of wire that connects the Network to the Local Area Network and passes all packets without redirecting any incoming packets.

Applicant has reviewed Kalajan and has been unable to locate in Kalajan any suggestion that a server program using a secure hypertext transfer protocol (i.e., Kalajan's Host 1, 2 or 3) be configured to listen for requests for secure hypertext transfer protocol sessions on an unusual port (i.e., that Kalajan's Host 1 port number, Host 2 port number or Host 3 port number should be set to a non-standard port number), much less an unusual port number that is normally used for some other type of server program. This is not surprising, since the packet redirection performed by Kalajan's Server 18 hides the Hosts' IP addresses and port numbers from Clients so modifying Kalajan so that the Hosts use unusual port numbers would serve no

purpose, not even the usual purpose of making it harder for clients to find a server.

In the office action at paragraph 4, the Examiner asserts that Kalajan "... teaches a method for delivering a message to the port of a destination based on the source port of the sender (Col 2 lines 37-47) ..." [emphasis added].

What Kalajan actually teaches in the cited language is "... delivering a message unit to a destination network resource ..." (i.e., Kalajan's Host 1, Host 2 or Host 3) "... based upon a source address of the message unit ..." (i.e., Kalajan's Client A source address 14a alone or together with source port number 12a, Client B source address 14b alone or together with source port number 12b, or Client C source address 14c alone or together with source port number 12c) where "...the source address can be the source IP address ... or the source IP address and source port number ..." (Col 2 lines 37-47). Thus, Kalajan teaches how packets sent from Kalajan's Client A, B or C to Kalajan's Server (18), which has no analog in Applicant's Claims 1-3 or 9-11, can be redirected by Kalajan's Server (18) based upon such packets' respective source addresses.

Conversely, Claims 1-3 and 9-11 concern configuring a server (i.e., Kalajan's Host 1, Host 2 or Host 3) to listen for secure hypertext transfer protocol sessions on a port number (i.e., Host 1 port number 31a, Host 2 port number 31b or Host 3 port number 31c) that is normally associated with a hypertext transfer protocol. Nothing in Claims 1-3 and 9-11 involves redirecting any incoming packets from any client on any basis, including but not limited to, source IP address or source IP address combined with source port number. Thus, while the portions of Kalajan cited by the examiner concern redirecting incoming packets based upon where the packets are from, the Applicant's invention concerns changing the port number (corresponding to Kalajan's Host 1 port number 31a, Host 2 port number 31b or Host 3 port number 31c) on which a server (corresponding to Kalajan's Host 1, Host 2 and Host 3) will listen for incoming session requests from any client, regardless of the source IP address and source port number of the client.

Consequently, Kalajan at Col 2 lines 37-47 appears to the Applicant to be completely irrelevant to a discussion of whether or not Kalajan discloses the invention of claims 1-3 and 9-11 or anything similar to claims 1-3 and 9-11. Nothing in Kalajan at Col 2 lines 37-47 teaches changing the Host 1 port number (31a), Host 2 port number (31b) or Host 3 port number (31c).

In addition, the Examiner appears to admit that Kalajan does not teach configuring a server program to listen for requests for HTTPS sessions on a port number associated with the HTTP protocol (i.e., port 80). See the office action at Page 3 paragraph 4 where the Examiner states:

“However, Kalajan does not teach the specific implementation of the method to redirect the Secure Hypertext Transfer Protocol (HTTPS)(Col 10 line 20) which using the port 443 to port 80, the Hypertext Transfer Protocol (HTTP).”

It appears that the Examiner attempts to limit that admission by stating in the office action at Page 3 paragraph 4 that:

“Nevertheless, Kalajan teaches the implementation of the method in the Internet environment and further using the HTTPS and HTTP for a particular application (Col 3 lines 10-22).

Applicant has read the above quoted sentence in the office action several times and has reviewed Kalajan at Col 3 lines 10-22 several times. Applicant remains unable to figure out what the Examiner was trying to say in the above quoted sentence or how the cited portions of Kalajan might possibly be relevant to Claims 1-3 and/or 9-11. Although various sentences in Kalajan at Col 3 lines 10-22 do include the noun phrases “Internet”, “HTTPS” and “transport protocols”, such noun phrases are not linked together in a manner that discloses or

suggests any element of Applicant's invention. Kalajan at Col 3 lines 10-22, the portions cited by the Examiner, sets forth the following claimed advantages of Kalajan's invention:

"Clients can access destination network resources through available transport protocols, even if these resources do not have proper network addresses, or where those addresses remain secret." (Col 3 lines 12-15). To the contrary, Applicant's invention merely changes the port (which corresponds to Kalajan's host port numbers 31a, 31b and 31c) on which a server (which corresponds to Kalajan's Hosts 1,2 and 3) listens for requests and does not affect the server's IP address (i.e., Kalajan's Host Addresses 30a, 30b and 30c), and does not involve any redirecting of any packets.

"Employees can access their own desktop computers, ordinarily not having proper IP addresses, over the Internet using existing remote access applications." (Col 3 lines 15-18) To the contrary, Applicant's invention would not permit an employee to access an employee's desktop computer over the internet unless such employee's desktop computer has a valid, routable IP address and is running a server for a secure hypertext transport protocol. This is because Applicant's invention has nothing corresponding to Kalajan's Server 18 that redirects incoming packets.

"By conducting remote access sessions through Internet transport protocols, existing Internet encryption protocols (e.g., SSL as part of HTTPS) can be added to such sessions without any modification of the underlying remote access applications." To the contrary, if an HTTPS server were configured using Applicant's invention, then any underlying remote access applications that use such HTTPS server would need to be modified to include express references to the unusual port number assigned to the HTTPS server.

(1-a-2) Kalajan fails to disclose configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, as (i) required by Claim 2 and (ii) contemplated by Claims 10 and 11. Since HTTPS is an example of a secure hypertext

transport protocol and HTTP is an example of a Hypertext Transport Protocol, the general discussion above for item 1-a-1 is fully applicable here.

(1-a-3) Kalajan fails to disclose configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443, as (i) required by Claim 3 and (ii) contemplated by Claims 10 and 11. Since HTTPS is an example of a secure hypertext transport protocol that normally uses port 443 and HTTP is an example of a Hypertext Transport Protocol that normally uses port 80, the general discussion above for item 1-a-1 is fully applicable here.

(1-b) Kalajan teaches away from elements of Claims 1-3 and 9-11.

(1-b-1) Kalajan teaches away from providing to clients information about the IP address and host port number of secure hypertext transport servers (which correspond to programs running on one or more of Kalajan's Hosts 1, 2 and 3). Kalajan at col 3 lines 28-32 teaches that "[t]he client does not require detailed information about the network location of the LAN resource: no translation details need to be given to the client, either in advance, or through the Internet, to allow access." This is true in the context of Kalajan's invention because Kalajan's server 18 (which has no analog in Applicant's invention) redirects packets from Kalajan's Client A, B or C to Kalajan's Hosts 1, 2 or 3 (any one of which could correspond to Applicant's secure hypertext protocol server) based upon message routing information contained in Kalajan's server 18 that is organized based upon the source addresses of Kalajan's Clients A, B and C. Conversely, nothing in Applicant's invention suggests or claims redirecting any incoming packets. Thus, in Applicant's invention, where Kalajan's redirecting Server 18 is replaced with a wire, Kalajan's Clients A, B and C must know host addresses 30a, 30b and 30c and host ports 31a, 31b and 31c to send requests for sessions to Kalajan's Hosts 1, 2 or 3.

(1-c) As discussed in the Application as published on page 12 paragraphs 0232 – 0236, Applicant's invention seeks to solve the following problem (the "Firewall Problem"): how can a

client computer use HTTPS to communicate securely with a server computer when such client computer is connected to the Internet through a firewall that blocks packets addressed to destination port 443 (the port number normally associated with HTTPS) but passes packets addressed to destination port 80.

The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem.

(1-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP).

A. The materials available at <http://ftp.monash.edu.au/pub/ap/Apache/ch01.htm>, <http://ftp.monash.edu.au/pub/ap/Apache/ch04.htm>, <http://ftp.monash.edu.au/pub/ap/Apache/ch05.htm>, <http://ftp.monash.edu.au/pub/ap/Apache/ch07.htm> (hereinafter, collectively, Apache), portions of which were provided to Applicant by the Examiner and copies of which are being filed with the Supplemental IDS filed on January 11, 2005, teach away from using port 80 for any protocol other than http and teach away from using ports 1-1024 as a nonstandard port for a server.

In Chapter 1 of Apache at Fig. 1.1 (page 3 of 11 when printed by Applicant), the www service (which uses http, the hyper text transfer protocol) is equated with port 80. This teaches away from the notion that port 80 should be used for other protocols, including without limitation SSL/https.

In Chapter 7 of Apache under the heading "Protecting Your Data from Outside Access" at "Caution" (which appears on page 29 of 38 when printed by Applicant),

in the context of discussing how to hide a non-secure/http server, says in relevant part:

“The second way to make your server less likely to be found is to run it on a nonstandard port. Ports can range from 0 to 65,535, so there is a wide range to choose from. Generally, the first 1024 are considered reserved ports.”

By pointing out how many ports are potentially available and observing that the first 1024 are considered reserved ports, Apache teaches away from moving any server to a non-standard port in the range from 0 to 1024. That range includes port 80 which is normally associated with HTTP / hyper text transfer protocol.

B. The Examiner printed and provided a copy of pages 1-4 of 17 of Running a Perfect Web Site with Windows – Chapter 5, hereinafter Windows (Chapter 5), available on the web at http://www.gsu.unibel.by/pub/perf_web/06r07632.HTM). The Examiner did not list this reference in the Notice of References Cited. A full copy of Windows (Chapter 5) is being filed with the Supplemental IDS filed on January 11, 2005.

The notice at the top of Windows (Chapter 5) says “Copyright © 1996” and is very similar to the notice at the top of Chapter 4 of Apache that was provided by the Examiner.

Windows (Chapter 5) at the bottom of page 3 says in relevant part:

“... Ports under 1024 are reserved for the most common types of Internet traffic, so it is recommended that you use a number above 1024 if you need an alternate port. ...”

(1-c-2) Applicant’s invention has unexpected, serendipitous or counter-intuitive

results. At the time of Applicant's invention, based upon materials such as Apache (if it was in fact published before Applicant's invention) and Windows (Chapter 5), one skilled in the art would have expected that changing the port number on which an HTTPS server listens for session requests would make it harder for clients to communicate with such server. However, for clients connected to the Internet through certain types of firewalls, configuring an HTTPS server to listen on port 80 can make it possible for a client to establish an HTTPS session with such server in circumstances where it would not have been possible to establish an HTTPS session with such server if it were listening on port 443, the default port for HTTPS.

It is unexpected, serendipitous and counter-intuitive that configuring a server to listen to a non-standard and unexpected port would make it easier for some clients to reach such server, since this is precisely the sort of change that Apache and Windows (Chapter 5) teaches will make it harder for browsers to communicate with the server.

The unexpected, serendipitous and counter-intuitive results obtained by practicing the Applicant's invention cut strongly against the Examiner's view that Applicant's invention was obvious at the time it was made.

(1-c-3) During the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem (i.e., how to communicate securely through a firewall that blocks outgoing packets with a destination port of 443).

By rejecting Applicant's invention as obvious, the Examiner in essence contends that, at the time of Applicant's invention, it would have been obvious to one skilled in the art, when faced with the Firewall Problem addressed by Applicant's invention (i.e., that some clients are unable to communicate with a web server using HTTPS because such clients are connected to the Internet through a firewall that blocks packets to destination port 443), to

configure the destination web server to listen for requests for HTTPS sessions on port 80 and to direct the affected clients' browsers to request information using a resource locator of the form "https://www.domain.com:80".

The technical staff of every e-commerce web site that attempts to do business with the general public ought eventually to encounter the Firewall Problem since some customers and some potential customers spend some time at offices or other locations where their computers are connected to the Internet through firewalls that block outgoing packets addressed to destination port 443.

Consequently, if Applicant's invention should be obvious to anyone skilled in the art who encounters the Firewall Problem, then it would be logical to expect that, during the more than six years since Applicant first reduced Applicant's invention to practice and the more than three years since Kalajan issued, the technical staffs of many e-commerce web sites that seek to do business with the general public would either (i) have duplicated Applicant's invention or (ii) have settled upon some other solution to the Firewall Problem that permits secure communication with affected customers' computers.

However, Applicant is not personally aware of any web sites that direct a customer's browser to a resource locator of the form https://www.domain.com:80 or implement some other solution to the Firewall Problem that permits secure communication with customers' computers that are affected by the Firewall Problem.

Consider for example the web sites barnesandnobel.com and amazon.com – two popular, highly competitive, technologically savvy e-commerce web sites that seek to conduct business with the general public.

Based on tests conducted by Applicant on December 29, 2004, it appears that when confronted with the Firewall Problem, the persons skilled in the art employed by

barnesandnobel.com decided to drop back and punt. To ensure security, barnesandnobel.com uses SSL (i.e., HTTPS) for order submission and the collection of credit card information. If the computer used by a potential customer of barnesandnobel.com is connected to the Internet through a firewall that blocks outgoing packets addressed to destination port 443, then the potential customer is allowed to fill up a shopping cart but at checkout time the potential customer's browser will display an unhelpful error message as soon as the customer's browser is directed to establish an HTTPS session using the default destination port of 443.

Based on tests conducted by Applicant on December 28, 2004, it is clear that when confronted with the Firewall Problem, the persons skilled in the art employed by amazon.com have also failed to duplicate Applicant's invention or to implement some different solution that permits encrypted communication with affected customers. The folks at amazon.com clearly recognize the Firewall Problem, warn customers about it, and offer affected customers the choice of giving up or submitting order and payment details in an unsecured manner (i.e., using HTTP rather than HTTPS).

In particular, the last page of the check out process that amazon.com normally sends to customers without encryption (i.e., using HTTP) contains both a button labeled:

"Sign in using our secure server"

and a link that says

"The secure server will encrypt your information. If you received an error message when you tried to use our secure server, sign in using our standard server."

A copy of that page as viewed by the Applicant on December 28,

2004 is being filed with the Supplemental IDS filed on January 11, 2005. The above described button is a shaded oval near the middle of the web page (about 1/3 of the way down the printed page). The above described “standard server” link is near the bottom of the web page (a bit less than half-way down the printed page).

If a customer should click on the button labeled “Sign in using our secure server”, then such customer’s browser would be directed to a URL of the form “https://www.amazon.com/*”, which by default implies destination port 443. If such customer’s computer should be connected to the Internet through a firewall that blocks outgoing packets addressed to destination port 443 and such customer clicks on such button, then such customer would see an uninformative error message.

If a customer should click on the “standard server” link, then such customer’s browser would be directed to a URL of the form “http://www.amazon.com/*” which by default implies destination port 80, thereby avoiding part of the Firewall Problem. Unfortunately, since that URL begins with “http”, the remainder of the checkout process, including the transmission of credit card information, would then be conducted using HTTP which is NOT encrypted for security.

Since popular e-commerce sites that seek to do business with the general public neither (i) routinely use URLs of the form “https://www.securedomain.com/*:80” for the secure portions of their check out procedures nor (ii) routinely use some other solution to the Firewall Problem that ensures secure, encrypted communications with affected customers’ computers, Applicant contends that Applicant’s invention was not obvious when it was first reduced to practice by Applicant and remains non-obvious today, more than six years later.

(1-c-4) The Firewall Problem and Applicant’s invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server.

Applicant submits that one skilled in the art trying to figure out how to make it easier for clients to access a server would be highly unlikely to think that Kalajan's methods for making it harder to access a server would be relevant or helpful.

Thus, it would not have been obvious to one skilled in the art, seeking a solution to the Firewall Problem, and aware of Kalajan, that Kalajan was somehow relevant to solving the Firewall Problem.

(1-c-5) The Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem.

In the Office Action at page 3, paragraph 4, lines 2-5, the Examiner appears to admit that Kalajan does not teach configuring a server program to listen for requests for HTTPS sessions on a port number associated with the HTTP protocol (i.e., port 80) by stating:

“However, Kalajan does not teach the specific implementation of the method to redirect the Secure Hypertext Transfer Protocol (HTTPS)(Col 10 line 20) which using the port 443 to port 80, the Hypertext Transfer Protocol (HTTP).”

In the Office Action at page 3, paragraph 4, lines 5-10, the Examiner appears to attempt to address this component of the obviousness issue with the following language:

“Nevertheless, Kalajan teaches the implementation of the method in the Internet environment and further using the HTTPS and HTTP for a

particular application (Col 3 lines 10-22).

Therefore, it is obvious at the time of the invention for one of ordinary skill in the art to implement Kalajan's method to a mapping the https communication to the destination port 80.

Unfortunately, after carefully reviewing both Kalajan and the two sentences quoted immediately above, it is not at all obvious to Applicant what modifications to Kalajan the Examiner believes would bring Kalajan within the scope of any of claims 1-3 and 9-11.

The first of the two quoted sentences is not helpful to resolving the mystery because the cited portions of Kalajan, (i.e., Col 3 lines 10-22), do not have anything to do with configuring a server (i.e., Kalajan's Host 1, 2 or 3) to listen for requests for HTTPS sessions on an unusual port (i.e., changing Kalajan's Host 1 port number, Host 2 port number or Host 3 port number in any way, much less to port number 80). In particular, the cited portions of Kalajan describe the following claimed advantages of Kalajan's invention:

Kalajan at Col 3 lines 12-15 says "[c]lients can access destination network resources through available transport protocols, even if these resources do not have proper network addresses, or where those addresses remain secret." This does not have any relevance to changing any host's port number.

Kalajan at Col 3 lines 15-18 says "[e]mployees can access their own desktop computers, ordinarily not having proper IP addresses, over the Internet using existing remote access applications." This does not have any relevance to changing any host's port number.

Kalajan at Col 3 lines 18-22 says "[b]y conducting remote access sessions through Internet transport protocols, existing Internet encryption protocols (e.g., SSL as

part of HTTPS) can be added to such sessions without any modification of the underlying remote access applications.” This does not have any relevance to changing any host’s port number. In fact, by teaching no modification to applications, it seems to teach away from changing any host’s port number.

The second of the two quoted sentences is not helpful to resolving the mystery because the Examiner fails to set forth, or even to suggest, what changes to Kalajan’s method would cause Kalajan’s method to fall within any of (i) Claim 1 step (a), which requires configuring a server program so that it listens for requests for secure hypertext transfer protocol sessions on the port number normally associated with a hypertext transfer protocol rather than the port number normally associated with the secure hypertext transfer protocol, (ii) Claim 10, step (a), which requires configuring a web server system to use port 80 for secure communications or (iii) Claim 11, element (a), which requires web server software configured to use port 80 for secure communications.

In the Office Action at page 3, paragraph 4, lines 10-12, the Examiner goes on to say:

“The mapping port 80 to port 443 of the destination server create a diversion of traffic, which will the client accessing the information and at the same time protecting the information (Col 2 lines 12-35).”

Applicant does not find the sentence quoted immediately above to shed any light on what undisclosed modifications to Kalajan the Examiner believes would have been obvious. The portions of Kalajan cited in the above quoted sentence have nothing to do with changing any port numbers. Applicant is at a loss to understand why the Examiner believes that a discussion in Kalajan of ways to make it harder for clients to access Hosts would help explain how Kalajan could be modified to solve the Firewall Problem and make it easier for clients to use HTTPS to communicate with a host.

In the Office Action at page 3, paragraph 4, lines 12-13, the Examiner states, and Applicant admits:

“Further, it is well known in the art that HTTPS is using port 443 and Port 80 is using for HTTP.”

However, once again, this sentence sheds no light on how the Examiner proposes modifying Kalajan.

(1-d) The Examiner has failed to describe any modifications to Kalajan that the Examiner believes would bring Kalajan within the scope of all of Claims 1-3 and 9-11. The Examiner has failed to provide any prior art to support a view that it would have been obvious at the time of Applicant’s invention for one skilled in the art to modify Kalajan in such an undisclosed way. Applicant disagrees with the Examiner’s view that it would be obvious to one of ordinary skill in the art to make the undisclosed changes to Kalajan. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges the Examiner’s view and asks whether the Examiner can (i) describe a modification to Kalajan that would bring Kalajan within the scope of Claims 1-3 and 9-11 and (ii) show support for the view that it would have been obvious at the time of Applicant’s invention for one skilled in the art so to modify Kalajan.

In light of the foregoing discussion, Applicant respectfully requests that claims 1-3 and 9-11 be allowed.

The **Second Issue** is whether the Examiner is justified in rejecting Claim 4 under 35 USC 103(a) as being unpatentable over Kalajan, despite:

(2-a) Kalajan’s failure to disclose

(2-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and

(2-a-2) receiving at the server program on the port number associated with a hypertext

transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol;

(2-b) Kalajan's teaching away from

(2-b-1) providing to clients information about the IP address and host port number of secure hypertext transport servers and

(2-b-2) processing incoming packets differently based upon the destination port number to which they are addressed; and

(2-c) the fact that

(2-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(2-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(2-c-3) during the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem,

(2-c-4) the Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server, and

(2-c-5) the Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem; and

(2-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(2-a) Kalajan fails to disclose elements of claim 4.

(2-a-1) Kalajan fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by Claim 1 step (a), upon which Claim 4 depends. See the detailed discussion above at (1-a-1).

(2-a-2) Kalajan fails to disclose receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, as required by Claim 1 step (b) and Claim 4.

In the Office Action at page 3, paragraph 5, the Examiner incorrectly asserts that Kalajan discloses this required step at Col 4 lines 22-36.

The Examiner has failed to suggest any mapping between the elements of Kalajan's disclosure and the elements of Applicant's invention. After reviewing Kalajan, Applicant believes that the Examiner is suggesting the following mapping in the context of Claim 4:

Element of Kalajan's Disclosure	Element of Applicant's Invention
A program running on Kalajan's Host 1 (28a), Host 2 (28b) and/or Host 3 (28c)	Server Program using a secure hypertext transfer protocol
Kalajan's Host 1 port number (31a), Host 2 port number (31b) and/or Host 3 port number (31c)	Port number on which the Server Program Listens for requests for secure hypertext transfer protocol sessions
A program running on Kalajan's Client A (10a), Client B (10b) and/or Client C (10c)	Client Program
Kalajan's Server (18), which redirects packets based upon	The "system" of Claim 4.

the source address of the client that sent the packet to the Server	[While Applicant believes that this may be the mapping that the Examiner has in mind for the system of Claim 4, the Applicant disagrees with this mapping.]
---	---

Hypothetically, if the Examiner should be correct (which Applicant disputes), then Kalajan at Col 4 lines 22-36 would disclose, among other things, that Kalajan's Server 18 would pass to one of Kalajan's Hosts a data packet addressed to the port number associated with a hypertext transfer protocol but would block such data packet if it were addressed to the port number associated with a secure hypertext transfer protocol.

Applicant has carefully reviewed the cited portions of Kalajan, which discuss Kalajan's FIG 3. According to the cited portions of Kalajan, Kalajan's Server 18 determines the destination IP address and destination port number to which it will redirect an incoming packet based solely on the source IP address 14a of the Client 10 that sent the packet to Kalajan's Server 18. Thus, the portions of Kalajan cited by the Examiner teach that Kalajan's Server 18 will forward all packets received from a particular source IP address to a single Host at a single Host Port Number. Nothing in the language cited by the Examiner suggests in any way that the behavior of Kalajan's Server 18 will be different if the Client 10 addresses a packet to a different destination port.

(2-b) Kalajan teaches away from elements of Claim 4.

(2-b-1) Kalajan teaches away from providing to clients information about the IP address and host port number of secure hypertext transport servers. See the detailed discussion above at 1-b-1.

(2-b-2) Kalajan teaches away from processing incoming packets differently based upon the destination port number to which they are addressed. As discussed above in the context of 2-a-2, Kalajan at Col 4 lines 22-36 teaches that all incoming packets from a particular IP

address that are processed by Kalajan's server 18 (regardless of the IP address and port number to which such packets are addressed), should be redirected to the same Host destination address and Host destination port number.

(2-c) The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(2-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1.

(2-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-1.

(2-c-3) During the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(2-c-4) The Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server. See the discussion at 1-c-4.

(2-c-5) The Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem. With respect to Claim 1, see the discussion at 1-c-5. With respect to Claim 4, the Examiner has made no attempt to describe any modifications to Kalajan that would

bring Kalajan within the scope of Claim 4.

(2-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Kalajan to include, in combination, all of the elements of claim 4 that are missing from Kalajan, including, inter alia: (2-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (2-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext transfer protocol. Furthermore, the Examiner has failed to set forth modifications to Kalajan that would bring Kalajan within the scope of Claim 4. Applicant disagrees with the view that it would have been obvious to modify Kalajan in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear description of obvious changes to Kalajan that would bring Kalajan within the scope of Claim 4.

In light of the foregoing discussion, Applicant respectfully requests that Claim 4 be allowed.

The **Third Issue** is whether the Examiner is justified in rejecting Claim 5 under 35 USC 103(a) as being unpatentable over Kalajan despite:

(3-a) Kalajan's failure to disclose

(3-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and
(3-a-2) after so configuring the server, directing a client program to request information from the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated

with the hypertext transfer protocol;

(3-b) Kalajan's teaching away from

(3-b-1) providing to clients information about the IP address and host port number of secure hypertext transport servers;

(3-c) the fact that

(3-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(3-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(3-c-3) during the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem,

(3-c-4) the Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server, and

(3-c-5) the Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem; and

(3-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(3-a) Kalajan fails to disclose elements of Claim 5.

(3-a-1) Kalajan fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by Claim 1 upon which Claim 5 depends. See the detailed discussion above at 1-a-1.

(3-a-2) Kalajan fails to disclose, after so configuring the server, directing a client program to request information from the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol, as required by Claim 5. For example, but not by way of limitation, directing a browser on a client computer to request a URL of the form <https://www.domain.com:80>. [Please recall that https normally implies port 443 rather than port 80.]

In the Office Action at pages 3-4 paragraph 5, the Examiner incorrectly asserts that Kalajan teaches this element of Claim 5 at Col 4 lines 39-45 and Col 2 line 47. However:

Kalajan at Col 4 lines 39-45 states:

“Operating system (OS) 44 of server 18 receives messages having particular source address 14 and source port number 12, and passes those messages to their corresponding message delivery module 34, which, because of the mapping information received from address mapping table 38, then delivers those messages via LAN 26 to host 28a at host destination address 30a.”

Applicant has carefully examined the sentence quoted immediately above, and is unable to locate anywhere therein any disclosure or suggestion of directing a client program (i.e., a program running on one of Kalajan’s Clients A, B or C) to do anything, much less to request information from the server program (i.e., a program running on one of Kalajan’s Hosts 1, 2 or 3) using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol.

Kalajan's FIG. 4 makes it clear that Kalajan's Operating system (OS) 44, message delivery modules 34a, 34b and 34c are part of Kalajan's server 18. Kalajan's FIG. 2 makes it clear that Kalajan's Address Mapping Table 38 is also part of Kalajan's server 18. Consequently, the sentence quoted above concerns the internal operation of Kalajan's server 18. Unfortunately, the Examiner has failed to suggest, in the context of Claim 5, any mapping between Kalajan's server 18 and any element of Claim 5. Consequently, Applicant is at a loss to know whether or how the quoted sentence (which discusses the internal operation of Kalajan's server 18) is relevant in any way to Claim 5.

Kalajan at Col 2 lines 45-47 states:

"The source address can be the source IP address of the message unit, or the source IP address and source port number of the message unit."

Applicant has carefully examined the sentence quoted immediately above, and is unable to locate anywhere therein any disclosure or suggestion of directing a client program (i.e., a program running on one of Kalajan's Clients A, B or C) to do anything, much less to request information from the server program (i.e., a program running on one of Kalajan's Hosts 1, 2 or 3) using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol.

(3-b) Kalajan teaches away from Claim 5.

(3-b-1) Kalajan teaches away from providing to clients information about the IP address and host port number of secure hypertext transport servers. See the discussion above at 1-b-1.

Conversely, Claim 5 expressly requires both (i) configuring a server

program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (ii) directing a client program to request information from the server program using a resource locator comprising ... an indication to use the port number associated with the hypertext transfer protocol.

Applicant submits that directing a client program to issue a request that includes an unusual port number for a server program violates Kalajan's teaching that clients should not be provided information about the port numbers of hosts.

(3-c) The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(3-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1.

(3-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-1.

(3-c-3) During the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(3-c-4) The Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server. See the discussion at 1-c-4.

(3-c-5) The Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem. With respect to Claim 1, see the discussion at 1-c-5. With respect to Claim 5, the Examiner has made no attempt to describe any modifications to Kalajan that would bring Kalajan within the scope of Claim 5.

(3-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Kalajan to include, in combination, all of the elements of claim 5 that are missing from Kalajan, including, inter alia: (3-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (3-a-2) after so configuring the server, directing a client program to request information from the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol. Furthermore, the Examiner has failed to set forth modifications to Kalajan that would bring Kalajan within the scope of Claim 5. Applicant disagrees with the view that it would have been obvious to modify Kalajan in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear description of obvious changes to Kalajan that would bring Kalajan within the scope of Claim 5.

In light of the foregoing discussion, Applicant respectfully requests that Claim 5 be allowed.

The **Fourth Issue** is whether the Examiner is justified in rejecting Claim 6 under 35 USC 103(a) as being unpatentable over Kalajan, despite:

(4-a) Kalajan's failure to disclose

(4-a-1) configuring a server program to listen for requests for secure hypertext transfer

protocol sessions on a port number associated with a hypertext transfer protocol,
(4-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, and
(4-a-3) after so configuring the server, directing a client program to request information from the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol;

(4-b) Kalajan's teaching away from

(4-b-1) providing to clients information about the IP address and host port number of secure hypertext transport servers and

(4-b-2) processing incoming packets differently based upon the destination port number to which they are addressed;

(4-c) the fact that

(4-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(4-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(4-c-3) during the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem,

(4-c-4) the Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server, and

(4-c-5) the Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was

confronted by the Firewall Problem; and
(4-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(4-a) Kalajan fails to disclose elements of Claim 6.

(4-a-1) Kalajan fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by Claim 1 upon which Claim 4 depends upon which Claim 6 depends. See the detailed discussion above at 1-a-1.

(4-a-2) Kalajan fails to disclose receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, as required by Claim 1 step (b) and Claim 4, upon which Claim 6 depends. See the detailed discussion of this issue at 2-a-2.

(4-a-3) Kalajan fails to disclose, after so configuring the server, directing a client program to request information from the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol, as required by Claim 6. See the detailed discussion above at 3-a-2.

A. In the Office Action at page 4 paragraph 5, the Examiner incorrectly asserts that "... Kalajan discloses ... after step (a), directing a client program to request information from the server program using a resource locator (message directing application Col 4 line 14) comprising an indication to use the secure hypertext transfer protocol and an indication to use the second port number (Col 4 lines 37-45 and Col 6 lines 24-43)."

The Examiner has failed to set forth any mapping between the elements of Kalajan's disclosure and the elements of Applicant's invention. After reviewing Kalajan, Applicant believes that the Examiner is suggesting the following mapping in the context of Claim 6:

Element of Kalajan's Disclosure	Element of Applicant's Invention
A program running on Kalajan's Host 1 (28a), Host 2 (28b) and/or Host 3 (28c)	Server Program using a secure hypertext transfer protocol
Kalajan's Host 1 port number (31a), Host 2 port number (31b) and/or Host 3 port number (31c)	Port number on which the Server Program Listens for requests for secure hypertext transfer protocol sessions
A program running on Kalajan's Client A (10a), Client B (10b) and/or Client C (10c)	Client Program
Kalajan's Server (18), which redirects packets based upon the source address of the client that sent the packet to the Server	The "system" of Claim 4. [While Applicant believes that this may be the mapping that the Examiner has in mind for the system of Claim 4, the Applicant disagrees with this mapping.]

Using the mapping set forth immediately above, the Examiner's assertion is equivalent to asserting that Kalajan discloses directing a program running on Kalajan's Client A to request information from a program running on Kalajan's Host 1 using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with a hypertext transfer protocol.

Using the mapping set forth above, Kalajan's Server (18) is the system of Claim 4 and passes packets for which the destination port is associated with a hypertext transport protocol and blocks packets for which the destination port is associated with a secure hypertext transport protocol.

The Examiner cited Kalajan at Col 4 lines 13-15, which says:

“Referring also to FIG. 2, message routing application 24 includes port monitor 32, message delivery module 34 and dynamic table update module 36.”

Contrary to what the Examiner has suggested, the sentence quoted immediately above discloses nothing about directing a client program to do anything, directing a client program to request information, directing a client program to use a resource locator, directing a client program to use a resource locator comprising an indication to use a secure hypertext transfer protocol (or any other protocol), or directing a client program to use a resource locator that contains an indication to use the port number normally associated with a hypertext transfer protocol (or any other port number).

Furthermore, Kalajan’s FIG. 2 makes it clear that Kalajan’s message routing application 24, port monitor 32, message delivery module 34 and dynamic table update module 36 are all part of Kalajan’s Server 18. Using the mapping set forth above, this means that Col 4 lines 13-15 of Kalajan are describing the internal operation of the system of Claim 4 which blocks some incoming packets and passes others, based solely upon the destination port number specified in the incoming packets.

Since Kalajan at Col 4 lines 13-15 discusses structure that the Examiner in the context of Claim 4 suggested corresponds to the internal operation of the system of Claim 4, it makes no sense for the Examiner to assert in the context of Claim 6 that such language somehow concerns directing Kalajan’s Client A to do anything.

The Examiner cited Kalajan at Col 4 lines 37-46, which says:

“Message delivery module 34 handles all further communications between client 10 and host destination address 30a, in a manner

transparent to client 10. Operating system (OS) 44 of server 18 receives messages having particular source address 14 and source port number 12, and passes those messages to their corresponding message delivery module 34, which, because of the mapping information received from address mapping table 38, then delivers those messages via LAN 26 to host 28a at host destination address 30a.”

Contrary to what the Examiner has suggested, the sentence quoted immediately above discloses nothing about directing a client program to do anything, directing a client program to request information, directing a client program to use a resource locator, directing a client program to use a resource locator comprising an indication to use a secure hypertext transfer protocol (or any other protocol), or directing a client program to use a resource locator that contains an indication to use the port number normally associated with a hypertext transfer protocol (or any other port number).

Furthermore, Kalajan’s FIG. 2 makes it clear that Kalajan’s message delivery module 34, OS 44, and address mapping table 38 are all part of Kalajan’s Server 18. Using the mapping set forth above, this means that Col 4 lines 37-46 of Kalajan are describing the internal operation of the system of Claim 4 which blocks some incoming packets and passes others, based solely upon the destination port number specified in the incoming packets.

Since Kalajan at Col 4 lines 37-46 discusses functions that the Examiner in the context of Claim 4 suggested correspond to the internal operation of the system of Claim 4, it makes no sense for the Examiner to assert in the context of Claim 6 that such language somehow concerns directing Kalajan’s Client A to do anything.

The Examiner also cited Kalajan at Col 6 lines 24-43, which, in the

context of discussing FIG. 5 describes a message delivery method that involves changing entries in the address mapping table 38 (which is part of Kalajan's server 18 and, according to the mapping set forth above, part of the server of Claim 4).

Once again, since the cited portion of Kalajan discusses a method that the Examiner in the context of Claim 4 suggested corresponded to the internal operation of the system of Claim 4, it makes no sense for the Examiner to assert in the context of Claim 6 that such language somehow concerns directing Kalajan's Client A to do anything.

B. In the Office Action at page 4 paragraph 5 the Examiner states "Kalajan does have indication to use a specific port (Second Port) in the mapping table for network traffic to enter and exit (See Figure 1, Col 4 lines 54-64).

Applicant has carefully examined the sentence quoted immediately above and Kalajan's FIG. 1 and is unable to see any connection between them. Kalajan's FIG. 1 contains nothing labeled Second Port, mapping table or network traffic. Consequently, Applicant challenges the Examiner to explain how Kalajan's FIG. 1 supports the Examiner's assertion that Kalajan discloses directing a client program to do anything.

Kalajan at Col 4 lines 54-64 says:

"Each forked instance 34a, 34b and 34c of message delivery module 34 receives (from OS 44) only messages arriving respectively from clients 10a, 10b, 10c (having respective source addresses and port numbers). Each instance 34a, 34b, and 34c then delivers its respective messages to respective hosts 28a, 28b, and 28c. Another alternative, for a different type of OS (such as Windows), provides the message delivery module as a subroutine within message routing application 24, so that a new thread of the message delivery module subroutine is replicated for each

mapping.”

Contrary to what the Examiner has suggested, the language quoted immediately above discloses nothing about directing a client program to do anything, directing a client program to request information, directing a client program to use a resource locator, directing a client program to use a resource locator comprising an indication to use a secure hypertext transfer protocol (or any other protocol), or directing a client program to use a resource locator that contains an indication to use the port number normally associated with a hypertext transfer protocol (or any other port number).

Furthermore, Kalajan’s FIG. 4 makes it clear that Kalajan’s forked instances 34a, 34b and 34c of message delivery module 34, and OS 44 are components of Kalajan’s Server 18 while Kalajan’s FIG. 1 makes it clear that Kalajan’s message routing application 24 is also part of Kalajan’s Server 18. Using the mapping set forth above, this means that Col 4 lines 54-64 of Kalajan describe the internal operation of the system of Claim 4 which blocks some incoming packets and passes others, based solely upon the destination port number specified in the incoming packets.

Since Kalajan at Col 4 lines 54-64 discusses structure that the Examiner in the context of Claim 4 suggested corresponds to the internal operation of the system of Claim 4, it makes no sense for the Examiner to assert in the context of Claim 6 that such language somehow concerns directing Kalajan’s Client A to do anything.

C. In the Office Action at page 4 paragraph 5, the Examiner admits that Kalajan “... does not specifically use the https.” Based upon this admission, the Examiner then concludes “[t]herefore, it is obvious at the time of the invention for one of ordinary skill in the art to configure the specific port to be the https port to direct the traffic to the correct destination port on the destination server.”

Applicant has carefully considered the above quoted language from the Office Action, and has been unable to determine what changes to Kalajan's invention the Examiner believes would have been obvious.

Claim 6 requires directing a client program (e.g., a program running on Kalajan's Client A) to request information from the server program (e.g., an HTTPS server running on Kalajan's Host 1 that has been configured so that Host 1 Port Number 31a is equal to 80) using a resource locator comprising an indication to use the secure hypertext transfer protocol (e.g., <https://>) and an indication to use the port number associated with the hypertext transfer protocol (e.g., ":80").

The Examiner is suggesting that it would be obvious to modify Kalajan and "... configure the specific port to be the https port ...". What did the Examiner mean by the phrase "specific port"?

Since the relevant step of Claim 6 requires directing a program on Client A to do something, presumably the phrase "specific port" refers to Client A's source Port number 12a.

However, if one skilled in the art should for some reason decide to modify Kalajan by setting Client A's source Port number 12a equal to 443 (the default port number for the https protocol) as suggested by the Examiner, Kalajan as so modified still would not involve directing a client program (e.g., a program running on Kalajan's Client A) to request information from the server program (e.g., an HTTPS server running on Kalajan's Host 1 that has been configured so that Host 1 Port Number 31a is equal to 80) using a resource locator comprising an indication to use the secure hypertext transfer protocol (e.g., <https://>) and an indication to use the port number associated with the hypertext transfer protocol (e.g., ":80").

(4-b) Kalajan teaches away from elements of Claim 6.

(4-b-1) Kalajan teaches away from providing to clients information about the IP address and host port number of secure hypertext transport servers. See the detailed discussion above at 1-b-1.

(4-b-2) Kalajan teaches away from processing incoming packets differently based upon the destination port number to which they are addressed. See the detailed discussion above at 2-b-2.

(4-b-3) Kalajan teaches away from directing a client program to request information from the server program using a resource locator comprising an indication to use the port number associated with the hypertext transfer protocol.

Kalajan at Col 4 lines 37-39 says “Message delivery module 34 handles all further communications between client 10 and host destination address 30a, in a manner transparent to client 10.” [Emphasis added] For communication between the client and host destination address 30a to be transparent to the client, there must be no requirement that the client know either the host’s IP address 30a or the host’s port number 31a.

Conversely, Claim 6 requires directing a client program to request information from a program running on the host using a resource locator that comprises an indication to use the port number associated with the hypertext transfer protocol only after the program running on the host has been configured to listen for requests for secure hypertext protocol sessions on the same port number.

(4-c) The following points rebut the Examiner’s view that, at the time of Applicant’s invention, Applicant’s invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(4-c-1) At the time of Applicant’s invention, the state of the art was that one

seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1.

(4-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-1.

(4-c-3) During the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(4-c-4) The Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server. See the discussion at 1-c-4.

(4-c-5) The Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem. With respect to Claim 1, see the discussion at 1-c-5. With respect to Claim 4, the Examiner has made no attempt to describe any modifications to Kalajan that would bring Kalajan within the scope of Claim 4. With respect to Claim 6, see 4.a.3.

(4-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Kalajan to include, in combination, all of the elements of claim 6 that are missing from Kalajan, including, inter alia: (4-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, (4-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a

manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, and (4-a-3) after so configuring the server, directing a client program to request information from the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol. Furthermore, the Examiner has failed to set forth modifications to Kalajan that would bring Kalajan within the scope of Claim 6. Applicant disagrees with the view that it would have been obvious to modify Kalajan in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear description of obvious changes to Kalajan that would bring Kalajan within the scope of Claim 6.

In light of the foregoing discussion, Applicant respectfully requests that Claim 6 be allowed.

The **Fifth Issue** is whether the Examiner is justified in rejecting Claim 7 under 35 USC 103(a) as being unpatentable over Kalajan despite:

(5-a) Kalajan's failure to disclose

(5-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and

(5-a-2) after so configuring the server, directing a client program to post information to the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol;

(5-b) Kalajan's teaching away from

(5-b-1) providing to clients information about the IP address and host port number of secure hypertext transport servers;

(5-c) the fact that

(5-c-1) at the time of Applicant's invention, the state of the art was that one seeking to

use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(5-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(5-c-3) during the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem,

(5-c-4) the Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server, and

(5-c-5) the Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem; and

(5-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(5-a) Kalajan fails to disclose elements of Claim 7.

(5-a-1) Kalajan fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by Claim 1 upon which Claim 7 depends. See the detailed discussion above at 1-a-1.

(5-a-2) Kalajan fails to disclose, after so configuring the server, directing a client program to post information to the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol, as required by Claim 7. See the discussion above at 3-a-2, replacing "requesting information from" with "posting information to".

(5-b) Kalajan teaches away from Claim 7.

(5-b-1) Kalajan teaches away from providing to clients information about the IP address and host port number of secure hypertext transport servers. See the discussion above at 1-b-1.

Conversely, Claim 7 expressly requires both (i) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (ii) directing a client program to post information to the server program using a resource locator comprising ... an indication to use the port number associated with the hypertext transfer protocol.

Applicant submits that directing a client program to post information in a manner that includes an unusual port number for a server program violates Kalajan's teaching that clients should not be provided information about the port numbers of hosts.

(5-c) The following points rebut the Examiner's view that, at the time of Applicant's invention, Applicant's invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(5-c-1) At the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1.

(5-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-1.

(5-c-3) During the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed

since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(5-c-4) The Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server. See the discussion at 1-c-4.

(5-c-5) The Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem. With respect to Claim 1, see the discussion at 1-c-5. With respect to Claim 7, the Examiner has made no attempt to describe any modifications to Kalajan that would bring Kalajan within the scope of Claim 7.

(5-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Kalajan to include, in combination, all of the elements of claim 7 that are missing from Kalajan, including, inter alia: (7-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol and (7-a-2) after so configuring the server, directing a client program to post information to the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol. Furthermore, the Examiner has failed to set forth modifications to Kalajan that would bring Kalajan within the scope of Claim 7. Applicant disagrees with the view that it would have been obvious to modify Kalajan in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear description of obvious changes to Kalajan that would bring Kalajan within the scope of Claim 7.

In light of the foregoing discussion, Applicant respectfully requests that Claim 7 be allowed.

The **Sixth Issue** is whether the Examiner is justified in rejecting Claim 8 under 35 USC 103(a) as being unpatentable over Kalajan, despite:

(6-a) Kalajan's failure to disclose

(6-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol,

(6-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, and

(6-a-3) after so configuring the server, directing a client program to post information to the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol;

(6-b) Kalajan's teaching away from

(6-b-1) providing to clients information about the IP address and host port number of secure hypertext transport servers and

(6-b-2) processing incoming packets differently based upon the destination port number to which they are addressed;

(6-c) the fact that

(6-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(6-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(6-c-3) during the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely

duplicated Applicant's invention when confronted with the Firewall Problem,
(6-c-4) the Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server, and

(6-c-5) the Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem; and

(6-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(6-a) Kalajan fails to disclose elements of Claim 8.

(6-a-1) Kalajan fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by Claim 1 upon which Claim 4 depends upon which Claim 8 depends. See the detailed discussion above at 1-a-1.

(6-a-2) Kalajan fails to disclose receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, as required by Claim 1 step (b) and Claim 4, upon which Claim 8 depends. See the detailed discussion of this issue at 2-a-2.

(6-a-3) Kalajan fails to disclose, after so configuring the server, directing a client program to post information to the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol, as required by Claim 8. See the detailed discussion above at 3-a-2 and 4-a-3 (replacing "request information from" with "post information

to”).

(6-b) Kalajan teaches away from elements of Claim 8.

(6-b-1) Kalajan teaches away from providing to clients information about the IP address and host port number of secure hypertext transport servers. See the detailed discussion above at 1-b-1.

(6-b-2) Kalajan teaches away from processing incoming packets differently based upon the destination port number to which they are addressed. See the detailed discussion above at 2-b-2.

(6-b-3) Kalajan teaches away from directing a client program to post information to the server program using a resource locator comprising an indication to use the port number associated with the hypertext transfer protocol. See the detailed discussion above at 4-b-3, replacing “request information from” with “post information to”.

(6-c) The following points rebut the Examiner’s view that, at the time of Applicant’s invention, Applicant’s invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(6-c-1) At the time of Applicant’s invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1.

(6-c-2) Applicant’s invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-1.

(6-c-3) During the more than six years that have passed since Applicant first

reduced Applicant's invention to practice and the more than three years that have passed since Kalajan issued, others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(6-c-4) The Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but Kalajan is in the field of making it harder for clients to access a server. See the discussion at 1-c-4.

(6-c-5) The Examiner failed to describe modifications to Kalajan that in the view of the examiner both (i) would bring Kalajan within the scope of any relevant claim and (ii) would have been obvious to one skilled in the art who was aware of Kalajan and was confronted by the Firewall Problem. With respect to Claim 1, see the discussion at 1-c-5. With respect to Claim 4, the Examiner has made no attempt to describe any modifications to Kalajan that would bring Kalajan within the scope of Claim 4. With respect to Claim 8, the Examiner has made no attempt to describe any modifications to Kalajan that would bring Kalajan within the scope of Claim 8.

(6-d) The Examiner has provided no prior art to support the Examiner's view that it would have been obvious at the time of Applicant's invention for one skilled in the art to modify Kalajan to include, in combination, all of the elements of claim 8 that are missing from Kalajan, including, inter alia: (6-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, (6-a-2) receiving at the server program on the port number associated with a hypertext transfer protocol a first data packet that has passed through a system that is configured in a manner that would block the first data packet if it were addressed to the port number associated with a secure hypertext protocol, and (6-a-3) after so configuring the server, directing a client program to request information from the server program using a resource locator comprising an indication to use the secure hypertext transfer protocol and an indication to use the port number associated with the hypertext transfer protocol. Furthermore, the Examiner has failed to set forth

modifications to Kalajan that would bring Kalajan within the scope of Claim 8. Applicant disagrees with the view that it would have been obvious to modify Kalajan in some undisclosed way. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can both show support for this view and set forth a clear description of obvious changes to Kalajan that would bring Kalajan within the scope of Claim 8.

In light of the foregoing discussion, Applicant respectfully requests that Claim 8 be allowed.

The **Seventh Issue** is whether the Examiner is justified in rejecting Claims 1-3 and 9-11 under 35 USC 103(a) as being unpatentable over Apache despite:

(7-a) Apache's failure to disclose

(7-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol,

(7-a-2) configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, and

(7-a-3) configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443;

(7-b) Apache's teaching away from

(7-b-1) using port 80 for a protocol other than http, and

(7-b-2) using a port less than 1024 as an alternate port for a server;

(7-c) the fact that

(7-c-1) at the time of Applicant's invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP),

(7-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results,

(7-c-3) during the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the approximately eight years that have passed since

the date of the copyright notice in Apache (i.e., 1996), others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem,

(7-c-4) the Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but the disclosure in Apache that teaches changing a servers port number is in the field of making it harder for clients to access a server, and

(7-d) the absence of any statement by the Examiner of the basis for a view as to what one skilled in the art would do.

(7-a) Apache fails to disclose elements of Claims 1-3 and 9-11.

(7-a-1) Apache fails to disclose configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, as required by (i) Claim 1 step (a) (upon which claims 2-3 and 9 depend), (ii) Claim 10 step (a) and (iii) Claim 11 element (a).

In the Office Action at page 5 paragraph 7 the Examiner appears to admit that Apache does not disclose configuring a server program in the required way when the Examiner states: "However, Apache does not teach the directives to set the port for https (443) to the same as http (80)."

Apache discusses web servers that use SSL and the secure sockets layer in Chapter 4. Applicant has diligently reviewed all of Chapter 4 of Apache, including portions not provided by the Examiner. The only discussion of secure hypertext communications (i.e., communication using SSL and the secure sockets layer) that Applicant could find in Chapter 4 of Apache is contained in the portions not provided by the Examiner. In particular, the discussion of Apache SSL contained in Chapter 4 of Apache runs from the heading "Apache-SSL" (on page 9 of 12 when Applicant printed it) through the end of Chapter 4. Applicant could not find any text in Chapter 4 of Apache that discloses anything about changing the port associated with

Apache-SSL. From Chapter 4 of Apache it is impossible to determine whether Apache-SSL permits use of the port directive. Consequently, Chapter 4 of Apache fails to disclose anything about configuring the port associated with a server that uses SSL and supports HTTPS sessions.

It appears that the Examiner is of the view that configuring an HTTPS server to listen on any port, in particular port 80, to be obvious. However, as we have stated many times, the Examiner's references teach away from actually configuring an HTTPS server to listen on port 80. See *In re Baird* which states: "The fact that a claimed species or subgenus is encompassed by a prior art genus is not sufficient by itself to establish a *prima facie* case of obviousness." *In re Baird*, 16 F.3d 380, 382, 29 USPQ2d 1550, 1552 (Fed. Cir. 1994). Applying this case to the facts herein, the collection of all ports (0 to 65535) is the genus. Port 80 is the species. Obviousness requires more than a knowledge in the art of how to configure an HTTPS server to listen on a particular port; it requires a motivation to do so. Such motivation has not been shown.

(7-a-2) Apache fails to disclose configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP, as (i) required by Claim 2 and (ii) contemplated by Claims 10 and 11. Since HTTPS is an example of a secure hypertext transport protocol and HTTP is an example of a Hypertext Transport Protocol, the general discussion above for item 7-a-1 is fully applicable here.

(7-a-3) Apache fails to disclose configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443, as (i) required by Claim 3 and (ii) contemplated by Claims 10 and 11. Since HTTPS is an example of a secure hypertext transport protocol that normally uses port 443 and HTTP is an example of a Hypertext Transport Protocol that normally uses port 80, the general discussion above for item 7-a-1 is fully applicable here.

(7-b) Apache teaches away from Claims 1-3 and 9-11.

(7-b-1) Apache teaches away from using port 80 for a protocol other than http. In Chapter 1 of Apache at Fig. 1.1 (page 3 of 11 when printed by Applicant), the www service (which uses http, the hyper text transfer protocol) is equated with port 80. This teaches away from the notion that port 80 should be used for other protocols, including without limitation SSL/https.

(7-b-2) Apache teaches away from using a port less than 1024 as an alternate port for a server. In Chapter 7 of Apache under the heading “Protecting Your Data from Outside Access” at “Caution” (which appears on page 29 of 38 when printed by Applicant), in the context of discussing how to hide a non-secure/http server, says in relevant part:

“The second way to make your server less likely to be found is to run it on a nonstandard port. Ports can range from 0 to 65,535, so there is a wide range to choose from. Generally, the first 1024 are considered reserved ports.”

By pointing out how many ports are potentially available and observing that the first 1024 are considered reserved ports, Apache teaches away from moving any server to a non-standard port in the range from 0 to 1024. That range includes port 80 which is normally associated with HTTP / hyper text transfer protocol.

(7-c) The following points rebut the Examiner’s view that, at the time of Applicant’s invention, Applicant’s invention would have been obvious to anyone skilled in the art who encountered the Firewall Problem:

(7-c-1) At the time of Applicant’s invention, the state of the art was that one seeking to use an alternate port number for a server would be advised to use a port number other than 80 (the default port for HTTP). See the discussion at 1-c-1 and at 7-b.

(7-c-2) Applicant's invention has unexpected, serendipitous or counter-intuitive results. See the discussion at 1-c-1.

(7-c-3) During the more than six years that have passed since Applicant first reduced Applicant's invention to practice and the approximately eight years that have passed since the date of the copyright notice in Apache (i.e., 1996), others who are skilled in the art have not regularly and routinely duplicated Applicant's invention when confronted with the Firewall Problem. See the discussion at 1-c-3.

(7-c-4) The Firewall Problem and Applicant's invention are in the field of making it easier for a client to access a server, but the disclosure in Apache that teaches changing a server's port number is in the field of making it harder for clients to access a server. With respect to Applicant's invention, see the discussion at 1-c-4. With respect to Apache, consider the following:

The portion of Chapter 4 of Apache that was provided and highlighted by the Examiner (i.e., page 5 of 12 after the heading "httpd.conf") discusses changing the port number associated with a non-secure/http server to make a server "secret". The relevant paragraph says:

"For a number of reasons, however, you might want to run your [non-secure/http] server on a different port; for example, there is already a server running on port 80, or this is a server you want to keep "secret." (Though if there is sensitive information on this, you should at least do host-based access control, if not password protection.)

Similarly, Chapter 7 of Apache, under the heading "Protecting Your Data from Outside Access" (which appears on pages 28-29 of 38 when printed by Applicant), says in

relevant part:

“The second way to make your server less likely to be found is to run it on a nonstandard port.”

Furthermore, in the Office Action at page 5, paragraph 7, the Examiner asserts without evidence that “... it is obvious at the time of the invention for one of ordinary skill in the art to implement the port directive to listen to https port 443 connection through port 80 to hide the server from hacking (Chapter 4, Page 5, second paragraph).” However, the Examiner does not assert that it would have been obvious to one skilled in the art, who wished to make it easier for browsers to communicate with an https server, to use the port directive to cause the https server to listen on port 80 (rather than the expected port 443).

Applicant submits that one skilled in the art trying to figure out how to make it easier for clients to access a server would be highly unlikely to think that Apache, which teaches methods for making it harder to access a server, would be relevant or helpful.

(7-d) The Examiner has provided no prior art to support the Examiner’s view that it would have been obvious at the time of Applicant’s invention for one skilled in the art to modify Apache, despite Apache’s teaching away from such a modification, to include any of (7-a-1) configuring a server program to listen for requests for secure hypertext transfer protocol sessions on a port number associated with a hypertext transfer protocol, (7-a-2) configuring a server program to listen for requests for HTTPS sessions on a port number associated with HTTP or (7-a-3) configuring a server program to listen for requests for HTTPS sessions on port number 80 rather than port number 443. Applicant disagrees with this view. Motivated by the case of *In Re Ahlert and Kruger*, 165 USPQ 418 (CCPA 1970) Applicant hereby challenges this view and asks whether the Examiner can show support for this view.

In light of the foregoing discussion, Applicant respectfully requests that claims 1-3 and 9-

11 be allowed.

In light of the discussion above of the First through Eighth Issues, Applicant respectfully requests that claims 1-11 be allowed.

Respectfully submitted,

Carl Oppedahl
Attorney for Applicant
Reg. No. 32746
P O Box 5068
Dillon, CO 80435-5068
telephone 970-468-6600

A handwritten signature in black ink, appearing to read "Carl Oppedahl", written over a horizontal line.